International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol 1 Issue 5 October 2015

Study of Attacks, Routing Protocols and Security challenges in VANET

Shahanawaz Ahmad Siddiqi [1], Mr. Zaheer Uddin[2]
Mtech. Scholar[1], Assistant Professor Dept of E&C [2], ASCT Bhopal
Siddiqui.fine@gmail.com[1], zaheeruddin18@gmail.com[2]

ABSTRACT:- The recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular Ad hoc Networks are multihop networks with no fixed infrastructure. It comprises of moving vehicles communicating with each other. One of the main challenge in VANET is to route the data efficiently from source to destination. Designing an efficient routing protocol for VANET is tedious task. Also because of wireless medium it is vulnerable to several attacks. Since attacks mislead the network operations, security is mandatory for successful deployment of such technology. This survey paper gives brief overview of different routing protocols. Also attempt has been made to identify major security issues and challenges associated with different routing protocols.

Keywords: ***VANET, ITS, Routing Protocols, Security, Attack.***

1. INTRODUCTION

A wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. Mobile Ad Hoc Networks (MANETS) is a term coined for the continuously varying network topology handheld mobiles devices. Vehicular Ad Hoc Networks (VANETS) is one of its types. It deploys the concept of continuously varying vehicular motion. The nodes or vehicles as in VANETS can move around with no boundaries on their direction and speed. Vehicular adhoc network (VANET) involves vehicle to vehicle (V2V), vehicle to roadside (V2R) or vehicle to infrastructure (V2I) communication [1].VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless adhoc network to be formed between vehicles. Each vehicle comprises of hardware unit for determining correct location information using GPS. Roadside Units (RSUs) are placed across the road for infrastructure communication. The number of RSU to be used depends upon the communication protocol.

VANET provide assistance to vehicle drivers for communication and coordination among themselves in order to avoid any critical situation through Vehicle to Vehicle communication [2] e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. Due to the dynamic nature of nodes in VANET the routing of data packets is much complex. Several factors like the type of the road, daytime, weather, traffic density and even the driver himself affect the movements of vehicles on a road. Hence, the network topology change frequently, and the routing protocol used has to adapt itself to these instantaneous changes continuously.

The paper is organized in VII sections. In Section II we discuss about VANET Overview. Section III highlights some of the standards for wireless access in VANET communication. Section. IV provides an overview about VANET routing protocols. In Section V describes the types of attack in VANET and the section VI is classify the attacks in VANET. The Section VII is provides the ides about to do work against hole attack and at last The paper closes with a conclusion in Section VIII.

VANET Overview

Intelligent Transportation System (ITS) - In Intelligent Transportation Systems (ITS) [3], each vehicle broadcast the information to the vehicular network or transportation agency, which then uses this information to ensure safe and free-flow of traffic. The possible communication configurations in ITS are inter-vehicle, vehicle to roadside, and routing-based communications [4] all this configurations requires precise and up-to-date surrounding information.

Inter-vehicle Communication

Inter-vehicle communication support multi-hop multicast/broadcast over a multiple hops to a group of receivers. ITS is generally concerned with the activity on the road ahead and not on road behind.

Naive broadcasting and intelligent broadcasting [4] are the two message forwarding methods used in inter-vehicle communications Naive broadcasting believes on the periodic broadcasting of message, if the message is from a vehicle behind it then vehicle ignores the message, but if the message comes from a vehicle ahead then the receiving vehicle sends its own broadcast message to vehicle behind it. Due to the large number of messages, probability of message collision increases which lowers the message delivery rate and increases its time of delivery. The problem is overcome using intelligent broadcasting. It uses acknowledgment address limiting the number of messages broadcast for emergency events only.

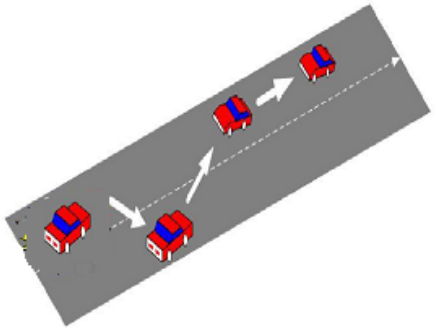

Fig.1. Inter-vehicle communication

Vehicle-to-roadside communication

In this type of communication, vehicle communication is done using single hop broadcasting method. This type of configuration provides ample amount of bandwidth link between communicating parties. In vehicle to roadside communication the maximum load for proper communication is given to the road side unit, it controls the speed of vehicle when it observes that a vehicle violates the desired speed limit, it delivers a broadcast message in the form of an auditory or visual warning, requesting the driver to reduce speed. Vehicle-to-roadside communication is shown in Fig. 2. Here RSU sends broadcast messages to all the equipped vehicles.

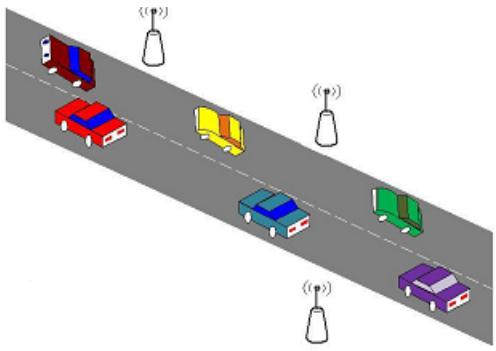

Fig. 2. Vehicle-to-Roadside Unit Communication

Routing-based communication

Multi-hop unicast method is used in routing-based communication configuration. While sending the message, the vehicle sends message using multi-hop fashion until it reaches to the desired vehicle. Receiving vehicle then sends a unicast message to the requested vehicle. Fig. 1 and Fig.2 shows the routing-based communication in VANET. Here any sender vehicle sends message to destination vehicle C using routing protocols. Standards for wireless access in VANET.

Standards for wireless access in VANET

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows: Fig. 2. Vehicle-to-Roadside Unit Communication.

Dedicated Short Range Communication (DSRC)

It provides a communication range from 300m to 1Km. The V2V and V2R communication takes place within this range. DSRC [5, 6] uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channel is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE)

It is also known as IEEE 802.11p. It supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz. frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. It contains the standard of IEEE 1609 [7, 8, 9]. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the signal into various narrow

band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels.

Routing Protocols Description

In MANET currently, there are mainly two types of routing protocols in MANETs, namely, topological routing and geographic routing [10, 11, 12]. In topological routing, mobile nodes utilize topological information to construct routing tables or search routes directly. In geographic routing, each node knows its own position and makes routing decisions based on the position of the destination and the positions of its local neighbors. The investigation of topological routing has lasted for decades, and a variety of topological routing protocols have been developed. Generally, the topological routing protocols can be further divided into two categories, namely, proactive routing and reactive routing. In proactive routing, route information is propagated periodically in the network.

Thus, each node can maintain a routing table containing route entries to other nodes. When packets arrive at an intermediate node, the next hop can be selected by looking up the routing table. Destination-sequenced distance-vector (DSDV) [7] routing is referred to as a well-known example of proactive routing. In reactive routing, no routing table is maintained at the nodes. When needed, the source node triggers a route search procedure to discover the routing path to the destination. Both ad hoc on-demand distance vector (AODV) [8] routing and dynamic source routing (DSR) [9] are referred to as representative examples of reactive routing. By exploiting the strength and avoiding the weakness of each type, hybrid topological routing protocols are proposed, for example, Zone Routing Protocol (ZRP) [10], which maintains a k-hop routing zone proactively and triggers the inter-zone route discovery reactively.

Types of attack in VANET

Attacks on Mobile Ad hoc Networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not [13, 14, 15].

Passive Attack

In passive attacks, an intruder the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect.

Active Attack

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks.

External Attack

External Attacks are carried by nodes that are not legitimate part of the network. In external attacks, it is possible to disrupt the communication of an organization from the parking lot in front of the company office.

Internal Attack

Internal Attacks are from compromised nodes that were once legitimate part of the network. In ad hoc wireless network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.

Attacks Classification

The types of attacks against can be classified is as follows:

Black Hole Attack - This is one of the security attack occur in VANET. In this attack the attacker node refuses to participate or even drop the data packet [16]. Hence the effect of this type of attack is most dangerous to the vehicular network.

Malware - Malware is a malicious software whose aim to disrupt the normal operation. This attack is carried out by insider. This attack is introduced in the network when the software update is received by car's VANET units and roadside station.

Broadcast Tampering - In this type of attack the attackers introduces false safety messages into the network. This message sometime hides the traffic warnings [17]. This leads to the critical situation like accidents and road congestions.

Spamming - Spamming are the messages which are of no use to the users like advertisements. The aim of such attack is to consume bandwidth and increase the transmission latency. Due to lack of centralized administration the controlling on such attack is difficult.

Greedy Drivers - Greedy drivers are those who try to attack for their own benefit. These drivers cause overload problem for RSU This leads to delay in service to the authorized users. On increasing number of such drivers the authorized users faced slow services.

Denial of Service - Denial of Service (DOS) [18] is one of the most serious level attacks in vehicular network. In DOS attack, the attacker jams the main communication medium and network is no more available to legitimate users. The main aim of DOS attacker is to prevent the authentic users to access the network services. DOS attack also causes the attacks like DDOS (Distributed Denial Of service) which is one of the sever attack in vehicular environment. The aim of this attack is to slow down the network. Jamming is also one of the kinds of DOS attack which jams the channel, thus not allowing other users to access the network services.

Replay Attack- This attack happens when an attacker replays the transmission of earlier information to take advantage of the situation of the message at time of sending [19].

Tunnelling - This attack happens when an attacker connects two distant parts of the Adhoc network using an extra communication channel as a tunnel. As a result, two distant nodes assume they are neighbours and send data using the tunnel [20]. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

Message Tampering - In this attack the valuable or even critical traffic safety messages can be manipulated. This is done by attacker by modifying, dropping or corrupting the messages [21].

EXPECTED OUTCOME

It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead In future we try to proposed a security scheme against hole attack through RSU unit that can collect and analyze audit data for the entire network. So according to that above definition we conclude MANET is distributed nature and can't trust to any of the mobile devices because we cannot manage the every time of topology changes on the network. This is very big challenge. So that particular point we create the trust based routing against the malicious attack in MANET.

CONCLUSION

In this paper various aspect of VANET like its environment, standards and network architecture has been discussed; furthermore various characteristics of VANET have been listed which distinguished it from other networks like MANET, Cellular, and WSN. Routing is an important component which used for more prominent and convenient communication. This paper includes detailed working and designing of various VANET routing protocols, finally various attacks in VANET have been classified depending on the availability, authentication, confidentiality, privacy, non repudiation and data trust. It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET. Since attack creates a more severe condition, it is necessary to analyze the effect of attack on routing protocols which makes more secure vehicular environment.

REFERENCES

[1] Kawashima, Hironao. "Japanese Perspective of Driver Information Systems."Transportation 17, no. 3 (1990): 263-284.

[2] [2] Harsch, Charles, Andreas Festag, and Panos Papadimitratos. "Secure position-based routing for VANETs." In Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, pp. 26-30. IEEE, 2007

[3] [3] Sun, Jinyuan, Chi Zhang, and Yuguang Fang. "An id-based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks." In Military Communications Conference, 2007. MILCOM 2007. IEEE, pp. 1-7. IEEE, 2007.

[4] [4] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular Ad hoc Networks (VANETs): status, results, and challenges." Telecommunication Systems (2010): 1-25.

[5] [5] Yin, Jijun, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. "Performance evaluation of safety applications over DSRC vehicular ad hoc networks." In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 1-9. ACM, 2004.

[6] [6] Guo, Jinhua, and Nathan Balon. "Vehicular Ad Hoc Network and Dedicated /short Range Communication Chapter. Available at link http://www. nathanbalon. com/project/cis95 (2006).

[7] [7] Z. J. Haas and M. R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," IEEE/ACM Trans. Net., vol. 9, no. 4, 2001, pp. 427–38.

[8] Jiang, Daniel, and Luca Delgrossi. "IEEE 802.11 p: Towards an international standard for Wireless access in Vehicular environments." In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pp. 2036-2040. IEEE, 2008.

[9] [9] IEEE (July 2007), "IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environment (WAVE)".

[10] [10] Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. Information Science Reference, 2010.

[11] [11] Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201 (2012)

[12] [12] Kumar, Rakesh, and Mayank Dave. "A Comparative Study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[13] [13] Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[14] [14] Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5. IEEE, 2011.

[15] Fuentes, José María de, Ana Isabel González-Tablas and Arturo Ribagorda. "Overview of security issues in Vehicular Ad-hoc Networks." (2010).

[16] 16] Sharma, Sheenu, Roopam Gupta, M. Tech Student Reader, RGPV SOIT, and RGPV UIT. "Simulation Study Of Blackhole Attack in the Mobile Ad hoc Networks." Executive Development 21 (2008).

[17] Krishnamurthi, Niyant, Anurag Ganguli, Abhishek, Tiwari, Bao-Hong Shen, Joseph Yadegar, and Gregory Hadynski. "Topology control for future airborne networks." In Military Communications Conference

[18] Ahmed Soomro, Irshad, Halabi Hasbullah, and Jamalul-lail Ab Manan. "Denial of Service (DOS) Attack and Its Possible Solution in VANET." (2010): 411-415.

[19] Parno, Bryan, and Adrian Perrig in , "Challenge in Securing Vehiclur Ad hoc Networks", In Workshop on Securing Vehicluar Communication in Wireless Topics in Networks (HotNets-IV), pp. 1-6. 2005.

[20] Panigrahi, Sunil Kumar, Soubhik Chakraborty, and Jibitesh Mishra. "A Statistical Analysis of Bubble Sort in terms of Serial and Parallel Computation." (2012).

[21] Leinmüller, Tim, Levente Buttyan, Jean-Pierre Hubaux,Frank Kargl, Rainer Kroh, Panagiotis Papadimitratos,Maxim Raya, and Elmar Schoch. "Sevecom-securevehicle communication." In Proceedings of IST Mobile Summit, vol. 2006. 2006.